Remarks

New claims 57–156 are submitted for the Examiner's consideration and are unrelated to the prosecution history of parent application.

Non-allowed claims 1-7, 9-15, 17-22, 24-28, 30-32, 34, 36-49 and 51-56 of the parent application are being submitted for reconsideration.

35 USC §103

The Examiner made statements (the first and last sentences of the paragraph bridging pages 3 and 4, the first sentence of the full paragraph of page 6, the last full sentence on page 7, the last sentence of the paragraph bridging pages 6 and 7, the first and last sentence of the last paragraph of page 9, the first sentence of the paragraph bridging page 11 and 12, the first and second to last sentence of the full paragraph of page 14, and the middle of the last full paragraph of page 17) such as, "It would have been obvious...to *allow* Nessett to combine with Minear" (emphasis added) and as such used the wrong criterion for obviousness. The Applicants note that obvious "to allow" to combine is a standard that is easier to prove than obvious "to try" to combine because "to allow" to combine implies a lack of a sufficient motivation to actually combine or even try to combine which is present in obvious "to try" to combine. The courts, however, have stated that obvious "to try" to combine is an insufficient standard of obviousness presumably because it is only a motivation to experiment rather than to actually combine and is a easier to meet than obvious to combine (see *In re Geiger*, 815 F.2d 686, 2 USPQ2d 1276 (Fed. Cir. 1987) for an example of a case in which "obvious to try" was

determined not to be obviousness). It logically follows that obvious "to allow" to combine is *a forte ore* also an insufficient criterion for obviousness under 35 USC §103.

Minear et al. relates to firewall-to-firewall connections. Minear et al.'s "invention is a system and method for regulating the flow of messages through a firewall" while in contrast Nessett et al. distributes the firewall.

The Examiner stated,

> Application gateway is known by definition as being software used to maintain security on a network.

However the phrase "application gateway" does not appear in Minear et al. Rather Minear et al. refer to an "application level gateway firewall 18." FIG. 1 labels feature number 18 as "FIREWALL." Thus the "application level gateway firewall" is just a long name for a firewall. Minear et al. and Nessett et al. discuss protecting unauthorized entry into nodes of repeaters and switches for example rather than unauthorized entry into applications and items associated with applications. The Applicants respectfully submit that the Examiner is apparently ignoring the word "application" in the phrase "application guard" of the independent claims, which implies that the securable component being guarded is in some way associated with an application.

The Examiner proposed "allowing" for a combined Nessett et al. and Minear et al. system. However, Nessett et al. states,

> Although products exist that provide for establishing security in particular product families, systems which take advantage of products in all the various categories of devices found in networks, require substantial administration. In a network involving a wide variety of network intermediate devices and terminals, an administrator is required to manage the establishment of security policy at all the various levels of protocol, and in all the various systems.

In other words Nessett et al. teach that the combined use of multiple security systems (e.g., that of Nessett et al. combined with Minear et al.) is difficult for an administrator to handle and should be avoided. Nessett et al. also states

> However, the variety of security features, and the various devices and levels of protocol at which they operate, present a significant administration problem to users of the security features. Because of the complexity, it is difficult to establish a coordinated security policy across all layers, and device types of the network, and particularly difficult to maintain such a system even if it could be successfully implemented.

Thus Nessett et al. in addition to trying to avoid using multiple security systems is trying to avoid having different security systems operating at different levels because of further administrative difficulties this creates. Minear et al.'s security system operates at the IP layer (the columns 3 lines 57-62). In contrast Nessett et al.'s system chooses the layer or layers at which to operate according to the components involved (column 3, lines 20-67). Nessett et al operates at multiple layers that are different at different parts of the system (column 4, lines 3-7) leading to a likelihood of having Minear et al. sometimes operating at a different layer than Nessett et al and sometimes operating at a common layer, thereby creating at least some places that generate the administrative difficulties Nessett et al. is trying to avoid and would be a move away from the coordinated security approach sought by Nessett et al.

Nessett et al. further teaches away from having redundancies (column 3, lines 64-67). Combining the system of Minear et al. with Nessett et al. would seem to be likely to result in undesirable redundancies at the IP layer.

Regarding claims 2, 3, 20, 39 and 40 the Examiner cited feature 11 of FIG. 1 and column 12, lines 34-37. However, the applicants respectfully submit that feature 11 of FIG. 1 and column 12, lines 34-37 do not explain any distribution mechanism. Claims 3,

20 and 40 specify a distributor for distributing the policy and further specify that the distributor is part of the policy manager. Even if Nessett et al. has a distributor it is not clear that it would be part of their policy manager, as required by claims 3, 20, and 40. Further feature 11 of FIG. 1 is a "network management station" rather than a "security management station" as specified by claims 2 and 39 from which claims 3 and 40 depend and as specified by claim 20. Column 12, lines 34-37 discuss a security policy "language" rather than a security policy (as in claim 2) or a global policy (as in claims 20 and 39) being edited via a management station as opposed to using a standard word processing editor to edit or write the source code. Possibly the systems administrator needs to edit the source code of a program that uses this language, and there is no security management station that allows for both editing and setting global or security policy. The Applicants respectfully request clarification as to how column 12, lines 34-37 imply or suggest the use of a security policy management station for both setting and editing global policy or security policy.

Regarding claims 11, and 37 the Examiner cited column 6, lines 12-34. However, column 6, lines 12-34 never mentions an application guard or authentication engine as required by claims 11 and 34 to be placed on a client server.

Regarding claims 6, 21 and 43, the "database management system" of column 9, lines 7-11, cited by the Examiner manages the "topology data base" of line 7 and is not a database management system of the claims. The topology database keeps track of the topology of the system as implied by its name. Thus the database management system (of line 8) is not for "maintaining" security policy as in claims 6, 21, and 43. Column 9, lines 23-27, cited by the Examiner, is under the heading of and therefore discusses the

"Security management back end" (column 9, line 16) rather than the database management system of line 8. The backend "translates" within the "context" of the topology database (column 9, lines 23-27). In other words the backend translates the policy using the topology database for the information about how the nodes are connected to one another rather than a database management system maintaining the security policy, as claimed.

Regarding claims 7, 28, and 46 the Examiner stated,

> Thus the security policy establishes configuration data in a repeater by updating a management node (column 12, lines 45-56).

The Applicants respectfully fail to see how the encryption of data sent between frames discussed in column 12, lines 45-56, cited by the Examiner, is related to optimizing the policy as claimed. Although encryption may enhance the impenetrability of the firewall, the policy relates to things such as whom can access which part of the system, for example, rather than the format used to send the data. Therefore encryption is not a way of optimizing the policy.

Regarding claims 9 and 25, the Examiner cited column 8, lines 7-14 and column 12, lines 26-31, however these lines do not address placing an additional application guard at each client as claimed.

It would appear that claim 19 should have been grouped with claims 9 and 25 rather than with claims 10, 26 and 36. Clarification is respectfully requested.

Regarding claims 10, 17, 26, 30, 36, and 47 the Examiner first asserts that the combination is obvious, next lists the features of the combination, then asserts that the two references are with in the same field of endeavor, and then concludes that "Accordingly" the combination would have been obvious. However, the Examiner failed

to provide a motivation for the combination. Alleging that two references are within the same field of endeavor does not provide a motivation for the combination.

Regarding claim 1, the Examiner stated that "the Application level gateway serve as a guard," while regarding claims 10, 19, 26, and 36 the Examiner stated, "all network traffic must pass through one of the proxies." It is not clear why the Examiner mentions the proxies. If the Examiner was trying to allege that the proxy is the application guard, he is contradicting his earlier allegation that the gateway firewall application 18 is the application guard. If the Examiner was alleging that the proxy is the claimed interface, then it is not clear why he mentioned the encryption interface. The encryption interface is not the interface of the claims because the interface of the claims is for requesting access to securable components while the encryption interface, "Crypto interface 80 [is] used to encrypt an IPSEC payload" (column 11, lines 46-48).

It would also appear that claim 34 should not have been grouped with claims 12, 24 and 44. The Applicants respectfully fail to see how the Examiner's discussion of claims 12, 24, 34 and 44 is relevant to claim 34. Clarification is respectfully requested.

Regarding claims 17, 30 and 47 eve if *arguendo* Minear et al. teach an application guard they clearly cannot teach an application guard that guards the policy manager (as opposed to one that guards other securable components) because the policy manager the Examiner relied upon is in Nessett et al.

Regarding claims 18 and 42 it is not seen where the Examiner finds a suggestion to use a local application guard that is distributed by the policy manager. The proxies of Minear et al. are not disclosed as being distributed locally implying that they are all located in the same location.

Regarding claim 53 and 54 column 6, lines 32-34, cited by the Examiner (towards the top of page 10), do not discuss the processor and therefore do not disclose the same processor distributing the policy and executing the policy manager.

The Examiner rejected claims 5, 14, 15, 22, 32, 41, 45, and 49 under 35 USC §103(a) as unpatentable over Nessett et al. in view of Minear et al. as applied to the above claims further in view of Abraham et al.

Regarding claims 5, 22, 32, 41, and 49, the Examiner cited column 7, lines 38-43 and column 9, lines 1-10 and then stated,

> By monitoring the user transactions the policy management administrator would be able to better customize policies. This would have motivated one of ordinary skill in the art to implement the modifications set forth above.

However, the Examiner never provides support for this statement. The motivation to combine or modify a reference must also have support. The Applicants hereby respectfully call upon the Examiner to provide support for this statement in accordance with 37 CFR 1.104 d(2)or provide a reference in accordance with the last sentence of the second paragraph of MPEP 2144.03.

The Applicants respectfully note that the Examiner's discussion of claims 5, 22, 32, 41, and 49 fail to explicitly address the "audit log" of claim 32.

The Examiner stated regarding claims 14, 15, and 45,

> It would be obvious to allow the combination of Nessett and Minear to implement the system taught by Abraham. This implementation would allow Nessett distribution system used by the administrator, to be controlled by menu sets. This would offer a more efficient means for network management of the security policy system.

However, the Applicants respectfully submit that the Examiner never provides support that efficiency is in anyway recognized to be related to menus. The Applicants

respectfully call for the Examiner to provide support for this statement under 37 CFR 1.104 d(2) or a reference in accordance the last sentence of the second paragraph of MPEP 2144.03.

The Examiner continued,

> One of ordinary skill in the art would have recognized that this combination would give the management abilities to analyze, edit, distribute and view audit log stored on the audit server.

However it is not clear that there is an audit log on an audit server in Abraham et al. It is not clear what would motivate the addition of an analyze option on the menu that Abraham never mentions, even assuming *arguendo* that it is present. It is not clear what support the Examiner has for the allegation that one of ordinary skill would have recognized that this combination would give management the ability to analyze and view an audit log. The Applicants respectfully call for the Examiner to provide support for these allegations under 37 CFR 1.140 d(2) or a reference in accordance the last sentence of the second paragraph of MPEP 2144.03.

Regarding claims 14, 15, and 45 the Examiner alleged that Nessett et al. teach the use of an "audit log" and cited column 13, lines 32-38. However, although Nessett et al. column 13, lines 32-38 state that

> repeaters ... can monitor port disconnects and reconnects, reporting these to network management applications,

Nessett et al. fail to state that the "disconnects" and "reconnects" monitored and reported are recorded in an audit log. The words record and log are absent from Nessett et al.'s specification.

It is not clear that the options provided in column 12, lines 15-44, cited by the Examiner, are in a menu format as required in the claims. It is not clear if Abraham et al.

provides a distributed policy option. Possibly the newly edited policy only gets distributed after closing the window and/or after rebooting the system or network. As the burden of establishing a prima fascia case of obviousness is upon the Examiner, it logically follows that the burden is upon the Examiner to establish that Abraham et al. suggest an explicit menu option of distributing policy.

Regarding claim 15, Abraham et al. never discloses a menu including all of the options listed, i.e., navigate tree, analyze policy, edit policy, distribute policy, and view audit log. In particular, none of the references cited teach or suggest a menu option of analyze policy or view audit log.

The Examiner rejected claims 13 and 27 under 35 USC §103(a) as unpatentable over Nessett et al. in view of Minear et al. as applied to claim 1 further in view of Rogers et al.

In making this rejection the Examiner stated,

> Rogers does not specifically teach the loader as being al [sic] loader for bulk policies. It would have been obvious to one of ordinary skill in the art to recognize that in the event of the administrator wanting to load numerous policies the policy management system would be equipped to handle such an occurrence.

In other words the Examiner first recognized that Rogers et al. lacks a teaching for the element (the bulk policy loader) missing from the modified device of Nessett et al. and first needs to modify Rogers et al. to have this missing component. After modifying Rogers et al. the Examiner stated,

> It would have been obvious ... to allow the combination system [that of Nessett et al. combined with Minear et al.] to implement the means of a policy loader as suggested by Rogers et al.

However, the policy loader of Rogers et al. is the wrong policy loader. In other words the Examiner is assuming that obvious to include a device, that does not actually exist but is

obvious over a second device, within a first device is obvious. The Applicants respectfully submit that the added level of foresight required to envision the modified second device that does not yet exist and the added foresight required to envision the behavior, potential benefits and pitfalls of this presently nonexistent device is beyond the standard of obviousness of 35 USC §103. The situation is somewhat analogous to a chess game. After any given move it can be argued that finding any and all of the next possible moves for a first player is obvious. The first player just needs to take each of his pieces one at a time and check each space along each possible direction of movement to find all possible next moves. Further after the next move has been made (no matter which move was chosen) to find all the possible moves of the next player is also likewise obvious by following the exact same process. Following this simple algorithm all possible game scenarios could be mapped out. Further, if the first player were to have all his possible game scenarios mapped out selecting which move gives the best outcome is also usually obvious. Yet, making the best next chess move is often far from obvious because of the tremendous foresight required to complete this sequence of obvious mappings and selections. Even selecting the move that will generate the best outcome were the game abruptly terminated after the next couple of moves is usually also far from obvious because of the foresight required. Likewise the foresight required to see all the possibilities after modifying a device to see the benefits and to see how to overcome potential obstacles in taking the nonexistent modified device and combining it with another nonexistent modified device is typically beyond obviousness.

The Examiner stated that combining the nonexistent modified device of Rogers et al. with the nonexistent modified device of Nessett et al. is bovious

> because Rogers teaches an invention similar to Nessett in that they both are directed towards policy management within a network system, and one of ordinary skill in the art would have recognized these similarities and concluded that they are form [sic] the same field of endeavor. This would have motivated one of ordinary skill in the art to implement the modifications set forth above.

In other words the Examiner alleged that (1) Rogers et al. and Nessett et al. are analogous art and (2) the motivation to combine these two nonexistent modified devices is that they are analogous art. However, the Applicants respectfully submit that the fact that two prior art devices are analogous art is not a sufficient motivation to combine to prove obviousness under 35 USC §103 but is just a prerequisite for using the prior art device in question.

Rogers et al.'s invention relates to administration systems (column 1, lines 10-14) and to policies for managing an entire system rather than policies that just apply one type of task such as enforcing security. Rogers et al.'s invention provides a policy implementation system that responds to changes in the network by providing threads representing event driven statements. The reason for doing this is because the written policy that would otherwise need to be implemented by operators often requires monitoring the state of the system. Rogers et al. discusses that implementation of policies often include complex rules for when to do which procedure. Rogers et al. further discuss that sequences of operations may change depending on the outcome of previous operations (column 1, lines 58-64). These problems are not very relevant to simpler policy managers such as those of Nessett et al., which just enforce access rights of workers, for example, and do not have many different types of sequences of operations that need to be changed depending on the outcome of other sequences of events. Consequently, the Applicants respectfully submit that Rogers et al. does not provide a

sufficient motivation for combining his device with that of Nessett et al., with or without their respective proposed modifications.

Further although column 12 lines 15-44 of Rogers et al. cited by the Examiner may mention changing the policy, it never discusses "loading" the policy as claimed. The word "load" and variations of it never appears in the text of Rogers et al. "Loading" a policy implies importing a policy that has already been entered somewhere (e.g. in a file) as opposed to merely being entered via keyboard directly into the program. Thus the combination proposed by the Examiner fails to suggest loading the policy, as claimed.

Summary

In numerous places the Examiner appears to use an improper standard of obvious to "allow" to combine as a standard of obviousness and implies that because two references are combinable or within the same field of endeavor therefore it is obvious to combine them, which is inconsistent with established case law.

In several places the Examiner provides motivations for combining references that are not found within the prior art. The Applicants respectfully request the Examiner to either provide support for these statements under 37 CFR 1.104 d(2) or provide a reference in accordance with the last sentence of the second paragraph of MPEP 2144.03.

Nessett et al. are trying to avoid redundancies and having multiple security systems operating at multiple levels both of which are likely outcomes of combining the security systems of Nessett et al and Minear et al., mitigating against making this combination in the manner proposed by the Examiner.

The Applicants have specifically pointed out several places the Examiner alleged certain features are disclosed by the references but upon a closer look the passages cited do not appear to fully support the Examiner's assertions. For example, the Applicant respectfully submit that it is not clear which claimed elements the Examiner believes correspond to which features of the references relied upon regarding the proxy, the encryption interface and the application level gateway. The proxies of Minear et al. are not disclosed as being distributed locally implying that they are all located in the same location. The Applicants respectfully submit that a topology management system is not the same as the claimed management system for maintaining security. Abraham et al. do

not disclose a menu including a log option and an analyze option. The Applicants respectfully request either a clearer explanation or withdrawal of the rejections affected.

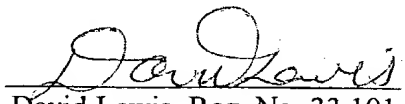
Regarding claims 13 and 27, the proposed modification of Nesset et al. with the modified device of Rogers et al. assumes that obvious to modify a first device with a non-existent second, where the nonexistent second device is an obvious modification of a third device, is obvious. However, the Applicants respectfully submit that in the present case more foresight is required than is justified under obviousness of 35 USC §103 for such a compound modification.

Rogers et al.'s concerns regarding changes in sequences of operations do not seem very relevant to the simpler system of Nesset et al. and therefore do not provide a sufficient reason for making the compound modification proposed by the Examiner.

In conclusion, Applicants respectfully submit that the claims are allowable, and therefore request that the Examiner withdraw the rejections and pass the application to issue. If the Examiner has questions regarding this case he is invited to contact Applicants' undersigned agent.

Respectfully submitted,

Richard Cappels et al.

Date: January 22, 2001 By: 

David Lewis, Reg. No. 33,101
Carr & Ferrell, *LLP*
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
Phone: (650) 812-3400
FAX: (650) 812-3444